TOP ATTACKS AND BREACHES

- The Louisiana Office of Motor Vehicles (OMV) and the Oregon DMV Services have released statements warning US citizens of a data breach exposing millions of driver's licenses. This comes after the Clop ransomware gang had hacked the agencies' MOVEit Transfer security file transfer systems and stole the stored data.

  Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat *((Progress MOVEit Transfer Multiple Vulnerabilities); Webshell.Win.Moveit, Ransomware.Win.Clop, Ransomware_Linux_Clop; Exploit.Wins.MOVEit)*

- The Swiss government has warned of ongoing DDoS attacks carried out by the Russian speaking hacktivist group NoName057(16) and effecting the Federal Administration websites. Around the same time the government has also disclosed that a ransomware attack by Play ransomware on the Swiss IT supplier Xplain is impacting its data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Play)*

- Ransomware group ALPHV claims to be behind the attack on Reddit, which was disclosed by the company during February 2023. The group claims to have stolen 80GB of data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats *(Ransomware.Win.BlackCat)*

- Researchers have found a new campaign aimed at infecting Windows and Linux systems with malware. The campaign is based on threat actors pretending to be cybersecurity researchers on social media platforms (Twitter, GitHub), publishing fake proof-of-concept exploits for zero-day vulnerabilities.

- Researchers have discovered a new ChromeLoader campaign that has been active since March 2023. This campaign targets visitors of pirated movie sites and infects them with a new variant of Shampoo – a search hijacker and adware browser extension.

  Check Point Threat Emulation provides protection against this threat *(Trojan.Win.ChromeLoader.A)*

- The Rhysida ransomware group has started leaking around 360K documents allegedly stolen from the network of the Chilean Army (Ejército de Chile), which had confirmed before that its systems were impacted in a security incident.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.

VULNERABILITIES AND PATCHES

- A third vulnerability (CVE-2023-35708) impacting the MOVEit Transfer application has been disclosed. The new flaw is a critical SQL injection vulnerability, now patched by Progress Software Company. Earlier this week, the company has warned its customers to restrict all HTTP and HTTPs traffic to MOVEit Transfer on their environment.

- Fortinet has shared information about a now patched critical heap-based buffer overflow vulnerability, dubbed XORtigate (CVE-2023-27997; CVSS score: 9.2), impacting FortiOS and FortiProxy SSL-VPN. The flaw has likely been exploited in the wild in attacks against the government, manufacturing, and critical infrastructure sectors.

  Check Point IPS provides protection against this threat *(Fortinet Multiple Products Heap-Based Buffer Overflow (CVE-2023-27997))*

- Microsoft has published June's Patch Tuesday with the total of 78 vulnerabilities addressed; six of them critical, 38 are listed as remote code execution vulnerabilities. None of the vulnerabilities are known to have been actively-exploited in the wild.

THREAT INTELLIGENCE REPORTS

- Check Point Research elaborates on the changes on PyPI, the official repository for Python packages, which is now suspending new users and projects registrations. This as a result of an attack with a seemingly harmless Python script can hide a malicious payload that can compromise a user's system.

  Check Point CloudGuard Spectral provides protection against this threat.

- Check Point provides details about the MOVEit vulnerability, its exploitation and the attack, as well as the major impact it had on variety of organizations across the world.

- CISA has shared a review of the LockBit ransomware, which was the most deployed ransomware in 2022. According to the report, since 2020 at least 1,700 US organization were attacked by the group and around $91M from US based victims alone were paid to the affiliates of Lockbit.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat.

- Researchers have found that a new version of GravityRAT, an Android remote access Trojan, is now enhanced with new capabilities, infecting mobile devices with a trojanized app named BingeChat. This is as a part of a new campaign active since August 2022, and aimed at stealing data from victims' devices.

- New details on Gamaredon Russia linked APT group, that consistently targets Ukraine, were revealed. Apart of regular infection chains, the group recently added to its arsenal a USB propagation malware.